Sysadmins' Round Table
7 October 2004

Image processing vulnerabilities

Widespread HEP community Linux compromises

Image Vulnerabilities

- jpg- and bmp-processing vulnerabilities have been found in Linux, MacOS X and Windows.
  - (Someone has been busy!)
- gdiplus.dll bug is particularly hard to eradicate, as versions of this file are distributed with *many* software products.

- **Exploits are out there.**

Widespread Compromises

- Labs and universities all around the world have been seeing intrusions on fully-patched systems.
- When local-exploit vulnerabilities, intruders get root access.
- Passwords gathered.
- Active remote login sessions hijacked.

Initial Intrusion

- The method of the initial intrusion is pretty irrelevant now, since this attack propagates along valid login paths.
  - Could have been any remote exploit: rpc, sshd, cvs, apache, weak passwords ... and anywhere in the world.
- Propagation is vastly amplified by systems with unpatched local vulnerabilities, such as mremap() or do_brk().

Attack Methods

- On a root-compromised machine, trojan versions of ssh and sshd gather passwords and private-key passphrases.
  - Stolen secrets are reported out in real time.
- Whether access is root or user-level, **appcap** can take temporary control of a network login client to access the remote host a user is connected to.

Appcap

- Appcap uses ptrace() to take control of a process such as an ssh client.
- It writes some machine code into the address space and makes the process run it.
  - Victim process' stdin & stdout reconnected to appcap's controlling terminal.
  - Upon ^C to appcap, stdin & stdout are restored.
  - Victim's session seems silent during hijack.

Exposure

- If someone can run under your uid on a given machine, they can hijack your remote sessions from that machine to others.
  - And so on, recursively.
- If someone is root on a given machine, they can do this to all users' sessions.
  - And so on, recursively.

Combatting the Intrusions

Impact on Fermilab

- Similar outbreaks in May 2003 & Spring 2004 only spread by captured passwords.
  - Fermilab escaped unscathed.
- This time:
  - Logins from CERN to FNAL were captured
    - Only Cryptocard responses!
  - Session from Spain to FNAL was hijacked.
    - No root access achieved!
    - Some writable web server cgi was altered.

Defenses

- Patches against local root exploits are vital.
  - Take a bow, system admins.
- Proper service (sshd) configuration.
  - Take a bow, CST
- Don't leave idle sessions around.
  - That slows the spread, but doesn't stop it.
- Don't forward tickets unnecessarily.
  - This may require unusual diligence.

More Defenses

- Disable WX access to memory.
  - Kernel work - feature exists in OpenBSD.
- Prevent ptrace().
  - Also have to restrict LKMs...